

## EXHIBIT B1

# Configuring Security

Created by ADMIN on 02/26/2013

When configuring security for your JIRA instance, there are two areas to address:

- permissions within JIRA itself
- security in the external environment

## Configuring permissions within JIRA

JIRA has a flexible security system which allows you to configure who can access JIRA, and what they can do/see within JIRA.

There are five types of security within JIRA:

1. [Global permissions](#) — these apply to JIRA as a whole (e.g. who can log in).
2. [Project permissions](#) — organised into permission schemes, these apply to projects as a whole (e.g. who can see the project's issues ('Browse' permission), create, edit and assign them).
3. [Issue security levels](#) — organised into security schemes, these allow the visibility of individual issues to be adjusted, within the bounds of the project's permissions.
4. [Comment visibility](#) — allows the visibility of individual comments (within an issue) to be restricted.
5. [Work-log visibility](#) — allows the visibility of individual work-log entries (within an issue) to be restricted. Does not restrict visibility of progress bar on issue time tracking.

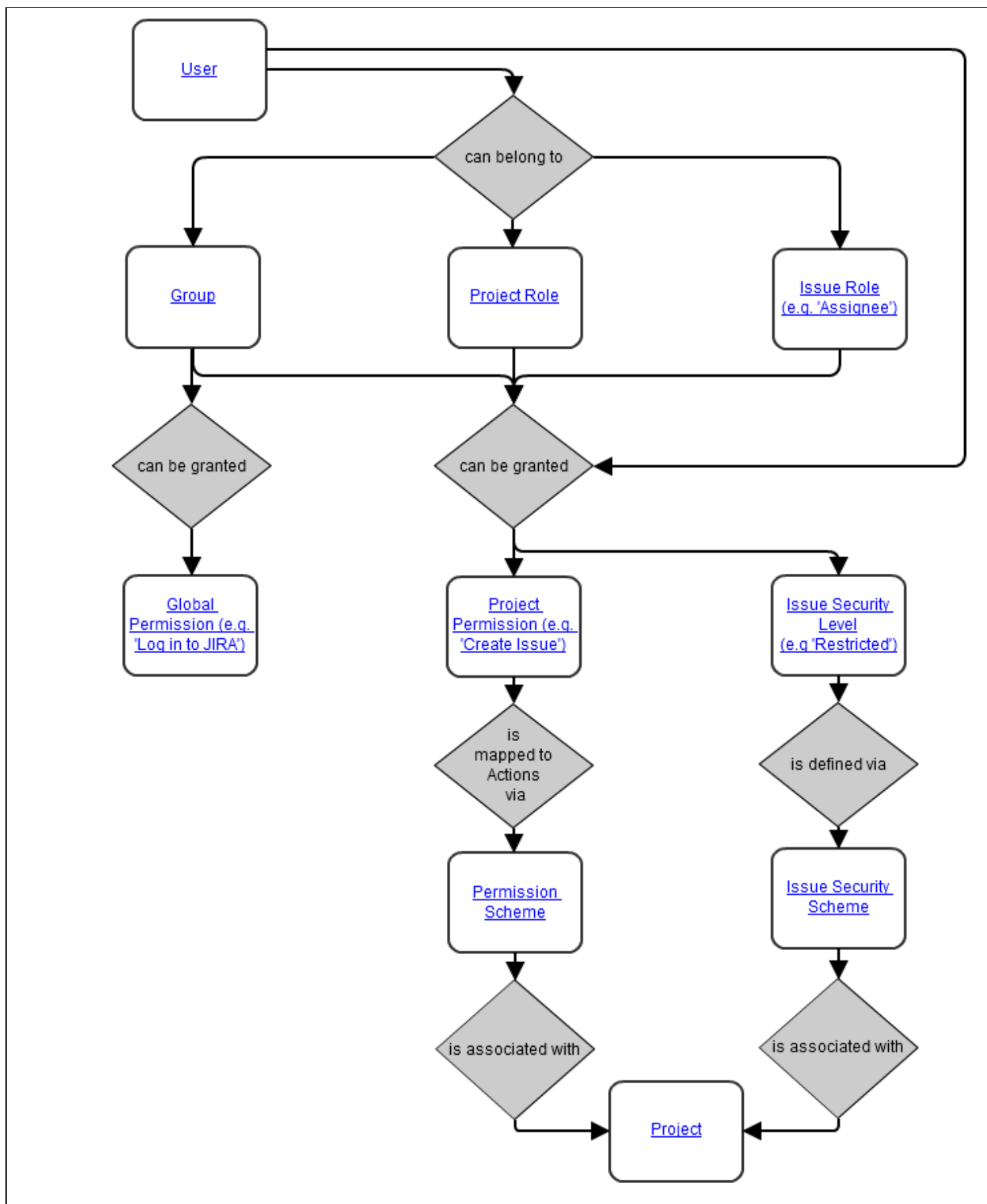
### On this page:

- [Configuring permissions within JIRA](#)
  - [Diagram: People and permissions](#)
- [Configuring security in the external environment](#)
- [Other security resources](#)

### In this section:

- [Configuring Issue-level Security](#)
- [Managing Project Permissions](#)
- [Managing Project Roles](#)
- [Managing Global Permissions](#)
- [Configuring Secure Administrator Sessions](#)
- [Preventing Security Attacks](#)
- [JIRA Cookies](#)
- [JIRA Admin Helper](#)
- [Password Policy for JIRA](#)


Diagram: People and permissions



## Configuring security in the external environment

---


If your JIRA instance contains sensitive information, you may want to configure security in the environment in which your JIRA instance is running. Some of the main areas to consider are:

 Unknown macro: 'conditionaltext'

- File system — you should restrict access to the following directories (but note that the user which your JIRA instance is running as will require full access to these directories):
  - [Index directory](#)
  - [Attachments directory](#)

## Other security resources

---

 Unknown macro: 'conditionaltext'

[Securing JIRA with Apache HTTP Server](#)

[JIRA Cookies](#)

[User and Group Management](#)

[Tomcat security best practices](#)

[Security Advisories](#)

[Configuring project specific security](#)

[Configuring Security](#)

[security](#)

[ssl](#)

[permissions](#)

[security-resources](#)

Powered by a free **Atlassian Confluence Open Source Project License** granted  
to NORTH TECOM . Evaluate Confluence today.

This Confluence installation runs a Free Gliffy License - Evaluate the Gliffy  
Confluence Plugin for your Wiki!